

# On the $k$ -error linear complexity for $p^n$ -periodic binary sequences via hypercube theory

Jianqin Zhou

Department of Computing, Curtin University, Perth, WA 6102 Australia  
Computer Science School, Anhui Univ. of Technology, Ma'anshan, 243002 China  
zhou9@yahoo.com

Wanquan Liu

Department of Computing, Curtin University, Perth, WA 6102 Australia  
W.Liu@curtin.edu.au

Guanglu Zhou

Dept of Mathematics & Statistics, Curtin University, Perth, WA 6102 Australia  
G.Zhou@curtin.edu.au

## Abstract

The linear complexity and the  $k$ -error linear complexity of a sequence are important security measures for key stream strength. By studying sequences with minimum Hamming weight, a new tool called hypercube theory is developed for  $p^n$ -periodic binary sequences. In fact, hypercube theory is very important in investigating critical error linear complexity spectrum proposed by Etzion et al. To demonstrate the importance of hypercube theory, we first give a general hypercube decomposition approach. Second, a characterization is presented about the first decrease in the  $k$ -error linear complexity for a  $p^n$ -periodic binary sequence  $s$  based on hypercube theory. One significant benefit for the proposed hypercube theory is to construct sequences with the maximum stable  $k$ -error linear complexity. Finally, a counting formula for  $m$ -hypercubes with the same linear complexity is derived. The counting formula of  $p^n$ -periodic binary sequences which can be decomposed into more than one hypercube is also investigated.

**Keywords:** *Periodic sequence; linear complexity;  $k$ -error linear complexity; hypercube theory*

**MSC2010:** 94A55, 94A60, 11B50

## I. INTRODUCTION

The linear complexity of a sequence  $s$ , denoted as  $L(s)$ , is defined as the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. The concept of linear complexity is very useful in the study of security of stream ciphers for cryptographic applications [1], [3]. In fact, the condition that the sequence has a high linear complexity is necessary for the security of a key stream. However, high linear complexity can not guarantee that the sequence is secure. For example, if a small number of changes to a sequence can greatly reduce its linear complexity, then the resulting key stream would be cryptographically weak. To tackle this issue, Ding, Xiao and Shan [1] proposed the weight complexity and sphere complexity. Stamp and Martin [12] introduced the  $k$ -error linear complexity, which is very similar to the sphere complexity. Specifically, suppose that  $s$  is a sequence with period  $N$ , for any  $k(0 \leq k \leq N)$ , the  $k$ -error linear complexity of  $s$ , denoted as  $L_k(s)$ , is defined as the smallest linear complexity when any  $k$  or fewer terms of the sequence are changed within one period.

One important result, proved by Kurosawa et al. [6] is that the minimum number  $k$  for which the  $k$ -error linear complexity of a  $2^n$ -periodic binary sequence  $s$  is strictly less than the linear complexity  $L(s)$  of  $s$  is determined by  $k_{\min} = 2^{W(2^n - L(s))}$ , where  $W(a)$  denotes the Hamming weight of the binary representation of an integer  $a$ .

For a  $p^n$ -periodic binary sequence, where  $p$  is an odd prime and 2 is a primitive root modulo  $p^2$ , Meidl [9] studied the minimum value  $k$  for which the  $k$ -error linear complexity is strictly less than the linear complexity. Han et al. [5] investigated the same issue in a new viewpoint different from the approach by Meidl [9]. In this paper, a more significant result will be presented using the proposed hypercube theory.

On the other hand, Etzion et al. [2] studied the error linear complexity spectrum of binary sequences with period  $2^n$ . They gave a precise categorization of those sequences having two distinct critical points in their spectra, as well as an enumeration of these sequences. We will extend these results over  $p^n$ -periodic binary sequences.

The literatures [2], [6], [7], [10], [12], [17], [18] concerning  $2^n$ -periodic binary sequences are mainly based on the Games-Chan algorithm [3] which efficiently computes the linear complexity of  $2^n$ -periodic binary sequences. In contrast, the literatures [5], [9] concerning  $p^n$ -periodic sequences are mainly based on the algorithm given by Xiao, Wei, Lam, and Imamura [14], which efficiently computes the linear complexity of  $p^n$ -periodic sequences. Generally, the latter is more complex to study.

The motivation of studying the stability of linear complexity is that changing a small number of elements in a sequence may lead to a sharp decline of its linear complexity. Therefore we really need to study such stable sequences in which even a small number of changes do not reduce their linear complexity. The stable  $k$ -error linear complexity is introduced to deal with this problem as follows. Suppose that  $s$  is a sequence over  $GF(q)$  with period  $N$ . For  $k(0 \leq k \leq N)$ , the  $k$ -error linear complexity of  $s$  is defined as stable when any  $k$  or fewer of the terms of the sequence are changed within one period, the linear complexity does not decline. In this case, the  $k$ -error linear complexity of sequence  $s$  is equivalent to its linear complexity.

By studying sequences with minimum Hamming weight, a new tool called hypercube theory is developed in this paper for  $p^n$ -periodic binary sequences. We first give a general hypercube decomposition approach. Second, a characterization is presented about the first decrease in the  $k$ -error linear complexity for a  $p^n$ -periodic binary sequence  $s$  based on hypercube theory. One significant benefit is to construct sequences with the maximum stable  $k$ -error linear complexity. Finally, A counting formula for  $m$ -hypercubes with the same linear complexity is derived. The counting formula of  $p^n$ -periodic binary sequences which can be decomposed into more than one hypercube is also investigated.

From the perspective of hypercube theory proposed, we can easily perceive the difficult points in solving the  $k$ -error linear complexity for a  $p^n$ -periodic binary sequence with more than one hypercube. This is the main contribution of this paper.

The rest of this paper is organized as follows. In Section II, some preliminary results are presented. Our main results are presented in Section III. The conclusions are given in Section IV.

## II. PRELIMINARIES

For definitions and notations not presented here, we follow [5], [9], [14]. In this section we give some preliminary results which will be used in the sequel.

Let  $x = (x_1, x_2, \dots, x_n)$  and  $y = (y_1, y_2, \dots, y_n)$  be vectors over  $GF(q)$ . Then we define

$$x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

If  $q = 2$ ,  $x + y$  is identical to  $x \oplus y$ .

Let  $q$  be a primitive root modulo  $p^2$  and  $s$  a  $p^n$ -periodic sequence over  $GF(q)$ .

$$s^{(n)} = \{s_0^{(n)}, s_1^{(n)}, s_2^{(n)}, \dots, s_{p^n-1}^{(n)}\}$$

is a period of  $s$ . The linear complexity of a  $p^n$ -periodic sequence can be efficiently obtained by the following XWLI algorithm [5], [14].

**Algorithm 2.1** Initially we put  $l = 0, L = 0$ . Let  $a = \{s_0, s_1, \dots, s_{p^n-1}\}$ . We will divide  $a$  into  $p$  equal parts,  $A_i = \{s_{ip^{n-1}}, s_{ip^{n-1}+1}, \dots, s_{(i+1)p^{n-1}-1}\}$ ,  $0 \leq i < p$ , then  $a = \{A_0, A_1, \dots, A_{p-1}\}$ .

For  $l < n$

- (i) if  $A_0 = A_1 = \dots = A_{p-1}$  then  $a \leftarrow A_0$  and  $l \leftarrow l + 1$ .
  - (ii) otherwise,  $a \leftarrow A_0 + A_1 + \dots + A_{p-1}$ ,  $l \leftarrow l + 1$ ,  $L \leftarrow L + (p-1)p^{n-l}$ .
- For  $l = n$   
 if  $A_0 \neq 0$ , then  $L \leftarrow L + 1$  and stop.  
 Finally, we have that  $L(s) = L$ .

Let  $q$  be a primitive root modulo  $p^2$  and  $s$  a  $p^n$ -periodic sequence over  $GF(q)$ . Han, Chung and Yang [5] showed that the linear complexity of  $s$  takes a value only from some specific ranges and can be expressed as

$$L(s) = \epsilon + (p-1) \sum_{v \in V} p^{v-1}$$

where  $V \subseteq \{1, 2, \dots, n\}$  and  $\epsilon \in \{0, 1\}$ .

For  $k(0 \leq k \leq N)$ , the  $k$ -error linear complexity of  $s$  is defined as stable when any  $k$  or fewer of the terms of the sequence are changed within one period, the linear complexity does not decline. In this case, the  $k$ -error linear complexity of sequence  $s$  is equivalent to its linear complexity. The following lemma is well known results on  $p^n$ -periodic binary sequences.

The number of  $p^n$ -periodic sequences with a given linear complexity value is computed by the DFT approach in [8].

**Lemma 2.1** Let  $q$  be a primitive root modulo  $p^2$  and  $s$  a  $p^n$ -periodic sequence over  $GF(q)$  with linear complexity  $L(s) = \epsilon + (p-1) \sum_{v \in V} p^{v-1}$ . Then the number of  $p^n$ -periodic sequence  $s$  is given by

$$N(L(s)) = \prod_{v \in V} (q^{(p-1)p^{v-1}} - 1)$$

where  $V \subseteq \{1, 2, \dots, n\}$  and  $\epsilon \in \{0, 1\}$ .

The following lemma is regarding to the sum of two sequences.

**Lemma 2.2** Let  $q$  be a primitive root modulo  $p^2$  and  $s_1$  and  $s_2$  sequences over  $GF(q)$  with period  $N = p^n$ . If  $L(s_1) \neq L(s_2)$ , then  $L(s_1 + s_2) > \min\{L(s_1), L(s_2)\}$ .

*Proof:* we give a proof based on Algorithm 2.1.

In the  $k$ th step,  $1 \leq k \leq n$ , if and only if  $A_0 = A_1 = \dots = A_{p-1}$  does not hold, then the linear complexity should be increased by  $(p-1)p^{n-k}$ .

Suppose that  $L(s_1) < L(s_2)$ , and in the computation of the linear complexity for  $s_2$ , the linear complexity is first increased by  $(p-1)p^{n-k_0}$ . Then in the computation of the linear complexity for  $s_1 + s_2$ , the linear complexity is also first increased by  $(p-1)p^{n-k_0}$ . Thus  $L(s_1 + s_2) > L(s_1) = \min\{L(s_1), L(s_2)\}$ .

The proof is complete now. ■

The following example is presented to illustrate Lemma 2.2.

For example, let  $s_1 = \{100 \ 100 \ 100\}$  and  $s_2 = \{010 \ 000 \ 000\}$ , where  $q = 2, p = 3$ . Then  $L(s_1) = 3, L(s_2) = 2 \times 3 + 2 + 1 = 9$  and  $L(s_1 + s_2) = 2 \times 3 + 2 = 8$ .

**Remark 2.1** Let  $s_1$  and  $s_2$  be binary sequences with period  $2^n$ . If  $L(s_1) \neq L(s_2)$ , then  $L(s_1 + s_2) = \max\{L(s_1), L(s_2)\}$ .

### III. HYPERCUBE THEORY

For the convenience of presentation, we introduce some definitions.

**Definition 3.1** Suppose that the position difference of two non-zero elements of sequence  $s$  is  $(px + i)p^y$ ,  $i \neq 0$ , where both  $x$  and  $y$  are non-negative integers, then the distance between the two elements is defined as  $p^y$ .

**Definition 3.2** Let 2 be a primitive root modulo  $p^2$ ,  $s$  a  $p^n$ -periodic binary sequence. When computing the linear complexity of  $s$  by Algorithm 2.1, if there is no decrease of nonzero elements in  $s$  in the operation

$a \leftarrow A_0 + A_1 + \cdots + A_{p-1}$ , (except for the last operation), then  $s$  is defined as a hypercube. The linear complexity of sequence  $s$  is defined as the linear complexity of hypercube  $s$ .

For example, let  $n = 3, p = 3, s^{(n)} = \{110\ 000\ 000\ 110\ 000\ 000\ 110\ 000\ 000\}$ . In the first operation  $a \leftarrow A_0 + A_1 + \cdots + A_{p-1}$ , from  $\{110\ 000\ 000\}$  to  $\{110\}$ , there is no decrease of nonzero elements. So  $s^{(n)}$  is a hypercube.

However, let  $n = 3, p = 3, s^{(n)} = \{110\ 100\ 100\ 110\ 100\ 100\ 110\ 100\ 100\}$ . In the first operation  $a \leftarrow A_0 + A_1 + \cdots + A_{p-1}$ , from  $\{110\ 100\ 100\}$  to  $\{110\}$ , there is a decrease of nonzero elements. So  $s^{(n)}$  is not a hypercube.

**Definition 3.3** A nonzero element of sequence  $s$  or a  $p$ -tuple  $\{A_0, A_1, \dots, A_{p-1}\}$  with even nonzero elements of sequence  $s$  is called a vertex, where  $A_i = \{s_{ip^j}, s_{ip^j+1}, \dots, s_{(i+1)p^j-1}\}$  and  $A_0 + A_1 + \cdots + A_{p-1} = 0, 0 \leq i < p, 0 \leq j < n$ .  $j$  is defined as the length of the vertex. Two vertexes can form an edge. If the distance between the two elements (vertices) is  $p^y$ , then the length of the edge is defined as  $p^y$ . If the number of vertices in a hypercube  $s$  is  $p^m$ , then hypercube  $s$  is called as  $m$ -hypercube, and the dimension of hypercube  $s$  is defined as  $m$ .

For example, let  $n = 3, p = 3, s^{(n)} = \{110\ 000\ 000\ 110\ 000\ 000\ 110\ 000\ 000\}$ . There are 3 vertices. So  $s$  is a 1-hypercube.

Based on Algorithm 2.1, we can have a standard hypercube decomposition of any sequence.

### Algorithm 3.1

**Input:**  $s^{(n)}$  is a binary sequence with period  $p^n$ .

**Output:** A hypercube decomposition of sequence  $s^{(n)}$ .

Step 1. Divide  $s^{(n)}$  into  $p$  equal parts,  $A_i = \{s_{ip^{n-1}}, s_{ip^{n-1}+1}, \dots, s_{(i+1)p^{n-1}-1}\}, 0 \leq i < p$ , then  $a = \{A_0, A_1, \dots, A_{p-1}\}$ .

Step 2. if  $A_0 = A_1 = \dots = A_{p-1}$  then we consider  $A_0$ .  $A_0$  is still a set of hypercubes, but the dimension of every hypercube reduced by 1.

Step 3. otherwise,  $a \leftarrow A_0 + A_1 + \cdots + A_{p-1}$ , then we consider  $A_0 + A_1 + \cdots + A_{p-1}$ . Some hypercubes of  $s^{(n)}$  may be removed. With these hypercubes removed recursively, we will obtain a series of hypercubes in the ascending order of linear complexity; while with these hypercubes left recursively, we will obtain a series of hypercubes in the ascending order of linear complexity.

Step 4. Finally, by restoring the dimension reduced of hypercubes, one can obtain a series of hypercubes in the ascending order of linear complexity.

We define it as **the standard hypercube decomposition** of sequence  $s^{(n)}$ .

For example, let  $n = 3, p = 3, s^{(n)} = \{110\ 100\ 100\ 110\ 100\ 100\ 110\ 100\ 100\}$ . Then it can be decomposed into 1-hypercube  $\{000\ 100\ 100\ 000\ 100\ 100\ 000\ 100\ 100\}$  and 1-hypercube  $\{110\ 000\ 000\ 110\ 000\ 000\ 110\ 000\ 000\}$ . They have linear complexity 6 and 8, respectively.

Based on Algorithm 2.1 and the standard hypercube decomposition, we first consider the linear complexity of a sequence with only one hypercube.

**Theorem 3.1** Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $s$  is an  $m$ -hypercube. If lengths of edges are  $p^{i_1}, p^{i_2}, \dots, p^{i_m}$  ( $0 \leq i_1 < i_2 < \dots < i_m < n$ ) respectively, then  $L(s) = \epsilon - 1 + p^n - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where if the vertex of hypercube is a nonzero element, then  $\epsilon = 1$ ; else if the length of the vertex is 0 then  $\epsilon = 0$ ; otherwise  $\epsilon = (1 - p)(p^0 + p^1 + \dots + p^{j-1})$ , where  $j$  is the length of the vertex.

*Proof:* In the  $k$ th step,  $1 \leq k \leq n$ , if and only if one period of the sequence can not be divided into  $p$  equal parts, then the linear complexity should be increased by  $(p - 1)p^{n-k}$ .

Suppose that non-zero elements of sequence  $s$  form a  $m$ -hypercube, lengths of edges are  $p^{i_1}, p^{i_2}, \dots, p^{i_m}$  ( $0 \leq i_1 < i_2 < \dots < i_m < n$ ) respectively. Then in the  $(n - i_m)$ th step, one period of the sequence can be divided into  $p$  equal parts, then the linear complexity should not be increased by  $(p - 1)p^{i_m}$ .

.....

In the  $(n - i_2)$ th step, one period of the sequence can be divided into  $p$  equal parts, then the linear complexity should not be increased by  $(p - 1)p^{i_2}$ .

In the  $(n - i_1)$ th step, one period of the sequence can be divided into  $p$  equal parts, then the linear complexity should not be increased by  $(p - 1)p^{i_1}$ .

Therefore,  $L(s) = \epsilon + (p - 1) + (p - 1)p + (p - 1)p^2 + \dots + (p - 1)p^{n-1} - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m}) = \epsilon - 1 + p^n - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ .

The proof is complete now. ■

**Example 3.1** Let  $n = 3, p = 3, s^{(n)} = \{110 \ 110 \ 110 \ 110 \ 110 \ 110 \ 110 \ 110\}$ .  $s^{(n)}$  is a 2-hypercube. Lengths of edges are  $3, 3^2$  respectively. The vertex of hypercube is  $\{110\}$ , not a nonzero element. The length of the vertex is 0. So,  $\epsilon = 0, L(s^{(n)}) = 0 - 1 + 3^3 - (3 - 1)(3 + 3^2) = 2$ .

**Example 3.2** Let  $n = 3, p = 3, s^{(n)} = \{000 \ 100 \ 100 \ 000 \ 100 \ 100 \ 000 \ 100\}$ .  $s^{(n)}$  is a 1-hypercube. The length of the edge is  $3^2$ . The vertex of hypercube is  $\{000 \ 100 \ 100\}$ , not a nonzero element. The length of the vertex is 1. So,  $\epsilon = -2, L(s^{(n)}) = -2 - 1 + 3^3 - (3 - 1)3^2 = 6$ .

Based on Algorithm 2.1, it is easy to give the following result about standard hypercube decomposition.

**Theorem 3.2** Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $L(s) = \epsilon - 1 + p^n - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ ,  $\epsilon \in \{0, 1\}$ , where  $0 \leq i_1 < i_2 < \dots < i_m < n$ , then the sequence  $s$  can be decomposed into several disjoint hypercubes, and only one hypercube has the linear complexity  $\epsilon - 1 + p^n - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , other hypercubes possess distinct linear complexities less than  $L(s)$ .

Let  $m(s)$  be the minimum  $k$  for which the  $k$ -error linear complexity is strictly less than the linear complexity of a given  $p^n$ -periodic binary sequence  $s$ . Let  $m_1(s)$  be the minimum  $k$  for which the  $k$ -error linear complexity is strictly less than  $L_{m(s)}(s)$ . We first consider sequences with only one hypercube.

**Theorem 3.3** Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $L(s) = \epsilon - 1 + p^n - (p - 1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where  $\epsilon \in \{0, 1\}$  and  $0 \leq i_1 < i_2 < \dots < i_m < n$ , and  $s$  is a hypercube. If hypercube  $s$  has  $lp^x, 0 < l < p$ , nonzero elements, then

$$m(s) = \begin{cases} lp^x, & l < p/2 \\ (p - l)p^x, & \text{otherwise} \end{cases}$$

If  $l > p/2$ , then  $m_1(s) = lp^x$ .

*Proof:* Based on Algorithm 2.1, to decrease the linear complexity of  $s$ , there are two possibilities.

If  $l < p/2$ , we have to remove the hypercube  $s$ . So  $m(s) = lp^x$ .

Otherwise, we have to add some nonzero elements to decrease the linear complexity of  $s$ . So  $m(s) = (p - l)p^x$ . In this case, in order to further decrease the linear complexity of  $s$ , we have to remove the hypercube  $s$ . So  $m_1(s) = lp^x$ . ■

The following examples are given to illustrate Theorem 3.3.

Let  $n = 3, p = 3, s^{(n)} = \{110 \ 000 \ 000 \ 110 \ 000 \ 000 \ 110 \ 000 \ 000\}$ . As hypercube  $s^{(n)}$  has  $2 \times 3$  nonzero elements and  $2 > 3/2$ , thus  $m(s^{(n)}) = (3 - 2)3 = 3, m_1(s^{(n)}) = 2 \times 3 = 6$ .

Let  $n = 2, p = 5, s^{(n)} = \{11110 \ 11110 \ 11110 \ 11110 \ 11110\}$ . Then  $L(s^{(n)}) = -1 + 5^2 - 4 \times 5$ . As hypercube  $s^{(n)}$  has  $4 \times 5$  nonzero elements and  $4 > 5/2$ , thus  $m(s^{(n)}) = (5 - 4)5 = 5, m_1(s^{(n)}) = 4 \times 5 = 20$ .

Let  $n = 3, p = 3, s^{(n)} = \{000 \ 100 \ 100 \ 000 \ 100 \ 100 \ 000 \ 100\}$ .  $s^{(n)}$  is a 1-hypercube.  $L(s^{(n)}) = -1 + 3^3 - (3 - 1)(1 + 3^2) = 6$ . As hypercube  $s^{(n)}$  has  $2 \times 3$  nonzero elements and  $2 > 3/2$ , thus  $m(s^{(n)}) = (3 - 2)3 = 3, m_1(s^{(n)}) = 2 \times 3 = 6$ .

For a  $p^n$ -periodic binary sequence  $s$ , Meidl [9] obtained sharp lower and upper bounds on  $m(s)$ . By Theorem 1 in [9], for  $s^{(n)} = \{11110 \ 11110 \ 11110 \ 11110 \ 11110\}$ ,  $m(s^{(n)}) \leq \frac{5-1}{2} \times 5^1 = 10$ .

By Theorem 1 in [9], for  $s^{(n)} = \{000 \ 100 \ 100 \ 000 \ 100 \ 100 \ 000 \ 100\}$ ,  $m(s^{(n)}) \leq \frac{3-1}{2} \times 3^2 = 9$ , which is even greater than  $m_1(s^{(n)})$ .

So the result obtained here is more precise.

The following theorem establishes a relationship between the greatest hypercube of  $s$  and  $m(s)$ .

**Theorem 3.4** Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $L(s) = \epsilon - 1 + p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where  $\epsilon \in \{0, 1\}$  and  $0 \leq i_1 < i_2 < \dots < i_m < n$ , and  $h$  is a hypercube with linear complexity  $L(s)$  in the standard hypercube decomposition of  $s$ . If hypercube  $h$  has  $lp^x$ ,  $0 < l < p$ , nonzero elements, then

$$m(s) = \begin{cases} lp^x, & l < p/2 \\ (p-l)p^x, & \text{otherwise} \end{cases}$$

If  $l > p/2$ , then  $m_1(s) = lp^x$ .

*Proof:* To decrease the linear complexity of  $s$ , we only need to consider hypercube  $h$  with linear complexity  $L(s)$ .

Based on Theorem 3.3, the result is obvious. ■

Now we consider an application of Theorem 3.4.

Let  $s$  be the binary sequence  $\{\overbrace{11 \dots 11}^{p^k} 0 \dots 0\}$ . Its period is  $p^n$ , and there are only  $p^k$  continuous nonzero elements at the beginning of the sequence. Then it is a  $k$ -hypercube, thus the  $p^{k-1}, \dots, (p^k - 2)$  or  $(p^k - 1)$ -error linear complexity of  $s$  are all  $p^n - (p^k - 1)$ .

After at most  $e$  ( $0 \leq e \leq p^k - 1$ ) elements of a period in the above sequence are changed, the linear complexity of all new sequences are not decreased, so the original sequence possesses stable  $e$ -error linear complexity.

So we have the following corollary.

**Corollary 3.1** For  $p^{l-1} \leq k < p^l$ , there exists a  $p^n$ -periodic binary sequence  $s$  with stable  $k$ -linear complexity  $p^n - (p^l - 1)$ , such that

$$L_k(s) = \max_t L_k(t)$$

where  $t$  is any  $p^n$ -periodic binary sequence.

It is worthy to mention that there are  $(3^{p^k})^{n-k}$  sequences with linear complexity  $p^n - (p^k - 1)$  from sequence  $\{\overbrace{11 \dots 11}^{p^k} 0 \dots 0\}$ . For example, let  $n = 2, p = 3$ . From  $s^{(n)} = \{111 \ 000 \ 000\}$ , we have the following  $3^3$  sequences with linear complexity  $3^2 - (3^1 - 1) = 7$ .

$$\begin{aligned} &\{111 \ 000 \ 000\}, \{011 \ 100 \ 000\}, \{011 \ 000 \ 100\} \\ &\{101 \ 010 \ 000\}, \{001 \ 110 \ 000\}, \{001 \ 010 \ 100\} \\ &\{101 \ 000 \ 010\}, \{001 \ 100 \ 010\}, \{001 \ 000 \ 110\} \\ &\dots \end{aligned}$$

Next we consider the construction of sequences with one or more hypercubes. Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $L(s) = \epsilon - 1 + p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where  $0 \leq i_1 < i_2 < \dots < i_m < n$ . We first derive the counting formula of  $m$ -hypercubes with the same linear complexity.

**Theorem 3.5** Suppose that  $s$  is a binary sequence with period  $p^n$ , and  $L(s) = \epsilon - 1 + p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where  $\epsilon \in \{0, 1\}$  and  $0 \leq i_1 < i_2 < \dots < i_m < n$ . Let

$$C = p^{p^m n - (p^m - p^{m-1})i_m - \dots - (p^2 - p)i_2 - (p-1)i_1 - \frac{p^{m+1} - p}{p-1}}$$

If sequence  $e$  is an  $m$ -hypercube with  $L(e) = L(s)$ , and the vertex in hypercube  $e$  is a nonzero element or the vertex is with length 0 and has  $l$  nonzero elements, then the number of sequence  $e$  is

$$\begin{cases} C, & \epsilon = 1 \\ \binom{p}{l} \left(\frac{C}{p}\right)^l, & \epsilon = 0 \text{ and } l \in \{2, 4, \dots, p-1\} \end{cases}$$

*Proof:* We first consider the case of  $\epsilon = 1$ .

Suppose that  $s^{(i_1)}$  is a  $p^{i_1}$ -periodic binary sequence with linear complexity  $p^{i_1}$  and  $W_H(s^{(i_1)}) = 1$ , then the number of these  $s^{(i_1)}$  is  $p^{i_1}$ .

So the number of  $p^{i_1+1}$ -periodic binary sequences  $s^{(i_1+1)}$  with linear complexity  $p^{i_1+1} - (p-1)p^{i_1} = p^{i_1}$  and  $W_H(s^{(i_1+1)}) = p$  is also  $p^{i_1}$ .

For  $i_2 > i_1$ , if  $p^{i_2}$ -periodic binary sequences  $s^{i_2}$  with linear complexity  $p^{i_2} - (p-1)p^{i_1}$  and  $W_H(s^{(i_2)}) = p$ , then  $p^{i_2} - (p-1)p^{i_1} - (p^{i_1+1} - (p-1)p^{i_1}) = (p-1)p^{i_2-1} + (p-1)p^{i_2-2} + \dots + (p-1)p^{i_1+1}$ .

Based on Algorithm 2.1, the number of these  $s^{i_2}$  can be given by  $(p^p)^{i_2-i_1-1} \times p^{i_1} = p^{pi_2-(p-1)i_1-p}$ .

(The following examples are given to illustrate the proof.

Suppose that  $i_1 = 1, i_2 = 3, p = 3$ , then  $(p^p)^{i_2-i_1-1} = 27$  sequences

{100100100 000000000 000000000},  
 {100100000 000000100 000000000},  
 {100100000 000000000 000000100},  
 {100000100 000100000 000000000},  
 {100000000 000100100 000000000},  
 {100000000 000100000 000000100},  
 {100000100 000000000 000100000},  
 {100000000 000000100 000100000},  
 {100000000 000000000 000100100},  
 .....

of  $s^{(i_2)}$  correspond to a sequence {100100100} of  $s^{(i_1+1)}$ .

So the number of  $p^{i_2+1}$ -periodic binary sequences  $s^{(i_2+1)}$  with linear complexity  $p^{i_2+1} - (p-1)(p^{i_2} + p^{i_1}) = p^{i_2} - (p-1)p^{i_1}$  and  $W_H(s^{(i_2+1)}) = p^2$  is also  $p^{pi_2-(p-1)i_1-p}$ .

For  $i_3 > i_2$ , based on Algorithm 2.1, if  $p^{i_3}$ -periodic binary sequences  $s^{i_3}$  with linear complexity  $p^{i_3} - (p-1)(p^{i_2} + p^{i_1})$  and  $W_H(s^{(i_3)}) = p^2$ , then the number of these  $s^{i_3}$  can be given by  $(p^{p^2})^{i_3-i_2-1} \times p^{pi_2-(p-1)i_1-p} = p^{p^2i_3-(p^2-p)i_2-(p-1)i_1-p-p^2}$ .

.....

So the number of  $p^{i_m+1}$ -periodic binary sequences  $s^{(i_m+1)}$  with linear complexity  $p^{i_m+1} - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m}) = p^{i_m} - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_{m-1}})$  and  $W_H(s^{(i_m+1)}) = p^m$  is also

$$p^{p^{m-1}i_m - \dots - (p^2-p)i_2 - (p-1)i_1 - p - p^2 - \dots - p^{m-1}}$$

For  $n > i_m$ , if  $p^n$ -periodic binary sequences  $s^{(n)}$  with linear complexity  $p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$  and  $W_H(s^{(n)}) = p^m$ , then the number of these  $s^{(n)}$  can be given by

$$\begin{aligned} & (p^{p^m})^{n-i_m-1} \times p^{p^{m-1}i_m - \dots - (p^2-p)i_2 - (p-1)i_1 - p - \dots - p^{m-1}} \\ &= p^{p^m n - (p^m - p^{m-1})i_m - \dots - (p^2-p)i_2 - (p-1)i_1 - p - \dots - p^{m-1} - p^m} \\ &= p^{p^m n - (p^m - p^{m-1})i_m - \dots - (p^2-p)i_2 - (p-1)i_1 - \frac{p^{m+1}-p}{p-1}} \end{aligned}$$

Now consider the case of  $\epsilon = 0$ .

Suppose that  $s^{(i_1)}$  is a  $p^{i_1}$ -periodic binary sequence with linear complexity  $p^{i_1} - 1$  and  $W_H(s^{(i_1)}) = l$ , then the number of these  $s^{(i_1)}$  is  $\binom{p}{l} p^{l(i_1-1)}$ .

So the number of  $p^{i_1+1}$ -periodic binary sequences  $s^{(i_1+1)}$  with linear complexity  $p^{i_1+1} - (p-1)p^{i_1} - 1 = p^{i_1} - 1$  and  $W_H(s^{(i_1+1)}) = lp$  is also  $\binom{p}{l} p^{l(i_1-1)}$ .

.....

Similarly, we have the following result.

If  $p^n$ -periodic binary sequences  $s^{(n)}$  with linear complexity  $p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m}) - 1$ , the vertex is with length 0 and  $W_H(s^{(n)}) = lp^m$ , then the number of these  $s^{(n)}$  can be given by

$$\binom{p}{l} \left(\frac{C}{p}\right)^l.$$

■

Suppose that  $s$  is a  $p^n$ -periodic binary sequence with more than one hypercube, and each hypercube has a fixed linear complexity. Now we consider the counting formula of these sequences. It should be noted that hypercubes are relatively independent. So after determining the connecting part of two hypercubes, one can construct each hypercube independently. Here we only give a special case of  $p^n$ -periodic binary sequence  $s$  with two hypercubes.

**Theorem 3.6** Suppose that  $s$  is a  $p^n$ -periodic binary sequence with two independent hypercubes:  $C_1, C_2$ .  $C_1$  has linear complexity  $p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , where  $0 \leq i_1 < i_2 < \dots < i_m < n$ , and  $C_2$  has linear complexity  $p^n - (p-1)(p^{j_1} + p^{j_2} + \dots + p^{j_l})$ , where  $0 \leq j_1 < j_2 < \dots < j_l < n$  and  $p^{j_1} > p^t$ , where  $t = \max\{x \mid i_x \leq j_1, x \geq 1\}$ . Then the number of sequence  $s$  is

$$\begin{aligned} & (p^{p^m n - (p^m - p^{m-1})i_m - \dots - (p^2 - p)i_2 - (p-1)i_1 - \frac{p^{m+1} - p}{p-1}}) \\ & [p^{p^l n - (p^l - p^{l-1})j_l - \dots - (p^2 - p)j_2 - (p-1)j_1 - \frac{p^{l+1} - p}{p-1}} (p^{j_1} - p^t)] \end{aligned}$$

*Proof:* The proof is very similar to that of Theorem 3.5.

Noted that  $s^{(j_1)}$  is a  $p^{j_1}$ -periodic binary sequence with linear complexity  $p^{j_1} - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_t})$  and  $W_H(s^{(j_1)}) = p^t$ , the number of zero elements in  $s^{(j_1)}$  is  $p^{j_1} - p^t$ .

Similar to the proof of Theorem 3.5, for each hypercube  $C_1$ , the number of hypercube  $C_2$  is

$$p^{p^l n - (p^l - p^{l-1})j_l - \dots - (p^2 - p)j_2 - (p-1)j_1 - \frac{p^{l+1} - p}{p-1}} (p^{j_1} - p^t)$$

This completes proof.

■

Suppose that  $s$  is a  $p^n$ -periodic binary sequence with two independent hypercubes:  $C_1, C_2$ .  $C_1$  has linear complexity  $p^n - (p-1)(p^{i_1} + p^{i_2} + \dots + p^{i_m})$ , and  $C_2$  has linear complexity  $p^n - (p-1)(p^{j_1} + p^{j_2} + \dots + p^{j_l})$ . Let  $\{x_1, x_2, \dots, x_y\} = \{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_l\}$ . Then it is easy to verify that  $L(s) = p^n - 1 - (p-1)(p^{x_1} + p^{x_2} + \dots + p^{x_y})$ .

For example, let  $n = 2, p = 3, C_1 = \{111 \ 000 \ 000\}$ ,  $L(C_1) = 3^2 - 2$ ,  $C_2 = \{100 \ 100 \ 100\}$ ,  $L(C_2) = 3^2 - 2 \times 3$ . Then  $s = \{011 \ 100 \ 100\}$ ,  $L(s) = 3^2 - 1 = 8$ .

#### IV. CONCLUSIONS

For a  $p^n$ -periodic binary sequence, where  $p$  is an odd prime and 2 is a primitive root modulo  $p^2$ , by studying sequences with minimum Hamming weight, a new tool called hypercube theory has been developed. A general hypercube decomposition approach has been given. Also, a characterization has been presented about the first decrease in the  $k$ -error linear complexity for a  $p^n$ -periodic binary sequence  $s$  based on the proposed hypercube theory. One very important application is to construct sequences with the maximum stable  $k$ -error linear complexity. Finally, A counting formula for  $m$ -hypercubes with the same linear complexity has been derived. The counting formula of  $p^n$ -periodic binary sequences which can be decomposed into more than one hypercube has been also investigated.

The hypercube structure of a  $p^n$ -periodic binary sequence is closely related to its linear complexity and  $k$ -error linear complexity. So it is very important in investigating critical error linear complexity spectrum proposed by Etzion et al, which is our future work.



## ACKNOWLEDGMENT

The research was partially supported by Anhui Natural Science Foundation(No.1208085MF106).

## REFERENCES

- [1] Ding, C.S., Xiao, G.Z. and Shan, W.J., The Stability Theory of Stream Ciphers[M]. Lecture Notes in Computer Science, Vol.561. Berlin/Heidelberg, Germany: Springer-Verlag, 1991,85-88.
- [2] Etzion T., Kalouptsidis N., Kolokotronis N., Limniotis K. and Paterson K. G., Properties of the Error Linear Complexity Spectrum, IEEE Transactions on Information Theory, 2009, 55(10): 4681-4686.
- [3] Games, R.A., and Chan, A.H., A fast algorithm for determining the complexity of a binary sequence with period  $2^n$ . IEEE Trans on Information Theory, 1983, 29 (1):144-146.
- [4] Fu F., Niederreiter H., and Su M., The characterization of  $2^n$ -periodic binary sequences with fixed 1-error linear complexity, In: Gong G., Hellesteth T., Song H.-Y., Yang K. (eds.) SETA 2006, LNCS, vol. 4086, 88-103. Springer (2006).
- [5] Han Y. K., Chung J. H., and Yang K., On the  $k$ -error linear complexity of  $p^m$ -periodic binary sequences. IEEE Transactions on Information Theory, 2007, 53(6): 2297-2304.
- [6] Kurosawa K., Sato F., Sakata T. and Kishimoto W., A relationship between linear complexity and  $k$ -error linear complexity. IEEE Transactions on Information Theory, 2000, 46(2): 694-698.
- [7] Lauder A. and Paterson K., Computing the error linear complexity spectrum of a binary sequence of period  $2^n$ . IEEE Transactions on Information Theory, 2003, 49(1):273-280.
- [8] Meidl W. and Niederreiter H., Linear complexity  $k$ -error linear complexity, and the discrete Fourier transform, J. Complexity, 2002, 18:87-103.
- [9] Meidl W., How many bits have to be changed to decrease the linear complexity?, Des. Codes Cryptogr., 2004, 33:109-122.
- [10] Meidl W., On the stability of  $2^n$ -periodic binary sequences. IEEE Transactions on Information Theory, 2005, 51(3): 1151-1155.
- [11] Rueppel R A. Analysis and Design of Stream Ciphers. Berlin: Springer-Verlag, 1986, chapter 4.
- [12] Stamp, M., and Martin, C. F., An algorithm for the  $k$ -error linear complexity of binary sequences with period  $2^n$ , IEEE Trans. Inform. Theory, 1993, 39:1398-1401.
- [13] Wei, S. M., Xiao, G. Z., and Chen, Z., A fast algorithm for determining the minimal polynomial of a sequence with period  $2p^n$  over  $GF(q)$ , IEEE Trans on Information Theory, 2002, 48(10):2754-2758.
- [14] Xiao, G. Z., Wei, S. M., Lam K. Y., and Imamura K., A fast algorithm for determining the linear complexity of a sequence with period  $p^n$  over  $GF(q)$ . IEEE Trans on Information Theory, 2000, 46: 2203-2206.
- [15] Zhou, J.Q., On the  $k$ -error linear complexity of sequences with period  $2p^n$  over  $GF(q)$ , Des. Codes Cryptogr., 2011, 58(3):279-296.
- [16] Zhou, J.Q., A counterexample concerning the 3-error linear complexity of  $2^n$ -periodic binary sequences, Des. Codes Cryptogr., 2012,64(3):285-286.
- [17] Zhou, J.Q., Liu, W.Q., The  $k$ -error linear complexity distribution for  $2^n$ -periodic binary sequences, Des. Codes Cryptogr., 2013, <http://link.springer.com/article/10.1007/s10623-013-9805-8>.
- [18] Zhu, F.X. and Qi, W.F., The 2-error linear complexity of  $2^n$ -periodic binary sequences with linear complexity  $2^n-1$ . Journal of Electronics (China), 2007,24(3): 390-395.